SISA

CUSTOMER SUCCESS STORY

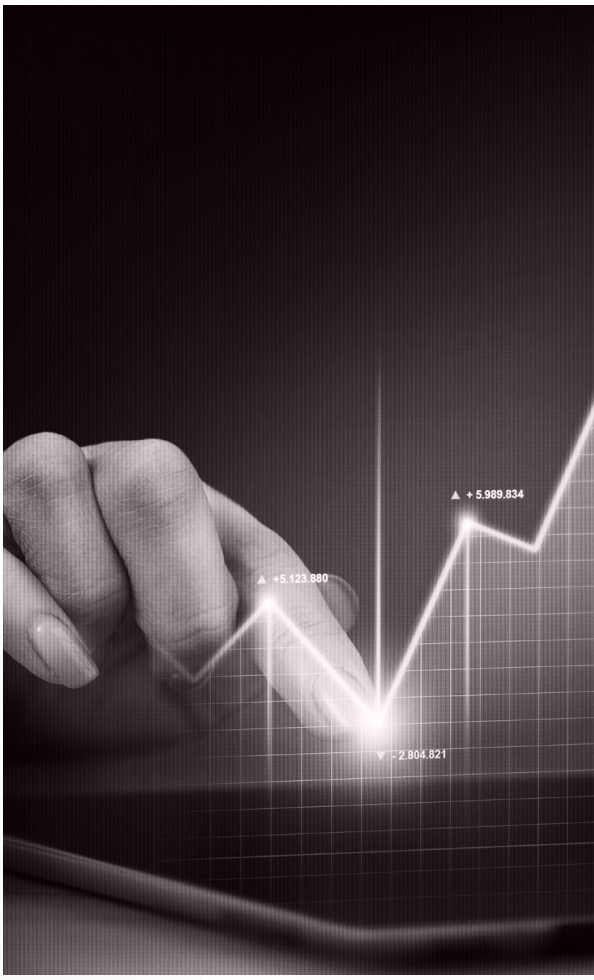
SISA's forensics-driven MDR solution helps Club Prophet improve monitoring of workloads on Google Cloud Platform

ABOUT THE CUSTOMER

Club Prophet Software LLC (referred to as Club Prophet) is one of the leaders in fully integrated golf management software systems. Founded in 1993 and headquartered in Oakmont, Pennsylvania, Club Prophet now operates in over 1,700 golf facilities of all types and sizes in 16 countries and 9 languages. The company's solutions have expanded to include food and beverage software, integration to external accounting programs, internet tee time options, integrated web store, lesson book, event management software, data collection kiosk, and a mobile iOS application for Apple iPads. As a leading technology provider to the golf industry, it provides full-service implementation, training and after-sale customer support to meet the end-to-end needs of the customers.

THE CHALLENGE

As a leading provider in the golf course management software space, offering a broad suite of solutions, Club Prophet was keen to focus on cybersecurity program to ensure compliance and improve monitoring of cloud environment. In particular, they were looking for a hybrid MFA-enabled MDR solution for their AWS environment (on-premises deployment), as well as a MDR solution hosted and managed by SISA (on SISA AWS), for monitoring Kubernetes workloads on their Google Cloud Platform (GCP). Secondly, they needed an asset integration mechanism for log forwarding from the GCP-hosted Kubernetes applications to SIEM server without deploying agents.



Club Prophet was also concerned about the proliferation of ransomware attacks looking to exploit security tooling and vulnerabilities in software applications. To secure their widespread digital touchpoints and ecosystem, they required a Managed Detection and Response (MDR) solution with customizable dashboards for real-time alerts and trends, email alert triggers for suspicious activities, and highly customized use cases for security monitoring. Lastly, compliance requirements and audits for the GCP environment were due, for which they were looking to engage with a PCI Qualified Security Assessor (QSA).

SOLUTION OFFERED BY SISA

To meet the PCI compliance regulations and keep up with the evolving threat landscape, Club Prophet needed to take a proactive approach and find a way to implement these controls efficiently. They decided to outsource the security tasks to a specialist MDR provider to augment their internal capabilities. A proof of concept gave them the opportunity to confirm that SISA was the best solution for their needs and would deliver the required security outcomes. Besides, they had previously engaged with SISA for carrying out PA DSS assessment and Vulnerability Assessment and Penetration Testing (VAPT) and were pleased with SISA team's expertise, level of support and the quality of service delivered.

SISA proposed 24/7 SOC Monitoring through a hybrid deployment of SISA ProACT MDR platform hosted on client's AWS account, and SISA AWS for Kubernetes applications on GCP. SISA's forensics-driven approach and consultative mindset provided the client's security team the confidence they needed to move forward. Thereafter, SISA's MDR team identified and created the process of forwarding the logs via the GCP Pub/Sub managed service for the Kubernetes applications hosted on client's GCP. SISA also provided customized agents for the critical server instances hosted on their AWS environment. The entire development and testing for GCP was done within two weeks while the full implementation in production was completed within a week.

CUSTOMER QUOTE

"Over the past several years, we have been using SISA's ProACT MDR services to meet PCI Compliance for 24/7 log monitoring. For our most recent certification, we decided to migrate the application to Google Cloud Platform's Kubernetes environment from an AWS + local application setup to improve reliability. Based on our requirement to support GCP, SISA's ProACT team worked with our developers to build a brand new custom SIEM application to fit our specific needs. The ProACT tool's custom alerting together with the MDR team's prompt actions has significantly improved our threat detection and response capability."

Karl Cavanaugh
Lead Security Analyst, Club Prophet Software LLC

The solution included the implementation and refinement of highly customized Use Cases for improved threat detection through SISA's USECASE Factory. SISA's team implemented 84 custom Use Cases developed using learnings derived from forensic investigations, to unlock advanced threat detection. Some of the custom Use Cases integrated into the ProACT platform included Pub/Sub topic modifications, Storage bucket modifications, IAM role modifications, Service Account Key modifications, Kubernetes role-binding modifications, and privilege escalations for GCP workloads and PowerShell executions, account privilege escalations, malicious registry changes for AWS workloads.

The other solution components of ProACT MDR service included:

- Quarterly Use Case simulations for all scenarios to test responsiveness and readiness for handling potential attacks.
- Integration of 60+ Threat Intel feeds for enhanced threat detection and enrichment.
- Daily Actionable Threat advisories to enable the client to pro-actively identify and address vulnerabilities.
- 24/7/365 monitoring of assets by SOC analysts.

BUSINESS IMPACT

SISA's Volume-based solution enabled 24/7 monitoring of hybrid assets while offering the client's team the flexibility to integrate assets from diverse environments. The platform's highly scalable architecture enabled the client to add higher volume of logs as per their requirements.

Club Prophet reported many benefits with this service such as improved detection accuracy, faster incident resolution time, reduced false positives, and improved compliance levels. Following the implementation of SISA ProACT solution, performance has improved across a number of key metrics:

- Mean Time to Detect (MTTD) has been reduced to 1 hour
- Mean Time to Respond (MTTR) has been reduced to 15 hours and
- False positives lowered to 10%

As a result of their partnership with SISA, Club Prophet has improved its security program alignment with compliance requirements and strengthened its preparedness for future audits. They successfully obtained PCI-DSS re-certification for their AWS, and PCI DSS certification for GCP environment for the first time. In addition, through sharing of actionable IOCs (Indicators of Compromise), Daily Threat Advisories, quarterly threat report and SISA Top 5 Forensic-driven Learnings Report, Club Prophet's overall security posture has improved significantly. As part of the ongoing engagement, the proposed migration of ProACT instance will lead to lower infrastructure costs and eliminate the need for regular maintenance, translating into higher ROI in the long term.

SISA

SISA is a global forensics-driven cybersecurity solutions company, trusted by leading organizations for securing their businesses with robust preventive, detective, and corrective cybersecurity solutions. Our problem-first, human-centric approach helps businesses strengthen their cybersecurity posture. We apply the power of forensic intelligence and advanced technology to offer true security to 2,000+ customers in 40+ countries.

Compliance

Payment Data Security

- PCI DSS
- PCI PIN
- PCI 3DS
- PCI P2PE
- PCI S3
- PCI S-SLC
- PCI CP (Card Production)
- Facilitated PCI SAQ
- Quarterly Health Check-ups
- Central Bank Compliance
- SWIFT

Strategy and Risk

- CCPA
- GDPR
- HIPAA
- ISO
- NIST
- SOC 1
- SOC 2
- Cloud Security

Security Testing

Application Security

- Application Penetration Testing
- CREST/CERT-in Approved Security Testing
- API Security Testing
- Secure Code Review

Network Security

- Vulnerability Assessment
- Penetration Testing
- Configuration Review
- Red Teaming Exercise
- Firewall Rule Review
- PCI ASV Scan
- Phishing Simulation

Hardware and IoT Security Testing

- Firmware Security Testing
- Hardware/Embedded Security Testing
- IoT Network Security Testing
- IoT/Embedded Application and Management Layer Security Testing

Cyber Resilience

Managed Detection and Response Solution – SISA ProACT

- Monitoring
- Attack Simulation
- Use-case Factory
- Advanced Threat Hunting

Digital Forensics and Incident Response

- Incident Response / Compromise Assessment Services
- Forensic Readiness Audit
- Forensic and Incident Response Retainer Service
- Payment Forensics Investigation
- Internal Forensics Investigation
- Ransomware Simulation

Data Governance

Data Discovery and Classification - SISA Radar

- Card Data Discovery
- PII (Privacy) Discovery
- Data Classification
- Data Masking/Encryption

Data Security as a Service

Cyber Academy

Payment Data Security Implementation

- CPISI
- CPISI Advanced
- CPISI-D (Developers)

Security Incident Detection and Response Programs

- CIDR

Cybersecurity Awareness

Forensic Learning Sessions for Senior Management

For more Information visit us at www.sisainfosec.com
OR
write to us at *contact@sisainfosec.com*

Follow us